(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4292869号
(P4292869)

(45)発行日　平成21年7月8日(2009.7.8)　(24)登録日　平成21年4月17日(2009.4.17)

(51)Int.Cl.		F I		
G06F 3/12	(2006.01)	G06F	3/12	K
B41J 5/30	(2006.01)	B41J	5/30	Z
B41J 29/38	(2006.01)	B41J	29/38	Z
G03G 21/04	(2006.01)	G03G	21/00	390
H04N 1/00	(2006.01)	H04N	1/00	C

請求項の数 7　(全 17 頁)

(21)出願番号　特願2003-151008(P2003-151008)
(22)出願日　平成15年5月28日(2003.5.28)
(65)公開番号　特開2004-355244(P2004-355244A)
(43)公開日　平成16年12月16日(2004.12.16)
審査請求日　平成18年2月23日(2006.2.23)

前置審査

(73)特許権者　303000372
コニカミノルタビジネステクノロジーズ株式会社
東京都千代田区丸の内一丁目６番１号
(74)代理人　100090033
弁理士　荒船　博司
(72)発明者　判治　精一
東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内
(72)発明者　角谷　正樹
東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内
(72)発明者　熊倉　俊一
東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内
最終頁に続く

(54)【発明の名称】画像形成装置

(57)【特許請求の範囲】
【請求項１】
印刷出力対象の出力データ及びユーザの第１の認証情報が記憶された記憶媒体を接続するためのインターフェイス部と、
ユーザの第２の認証情報を入力する認証情報入力部と、
前記第１のユーザの認証情報及び前記第２の認証情報に基づいて、ユーザの認証を行う第１制御部と、
前記記憶媒体に記憶された出力データの印刷が可能か否かを判断する第２制御部と、
前記第１制御部によりユーザが認証され、かつ前記第２制御部により印刷可能と判断されると、前記記憶媒体に記憶された出力データを前記記憶媒体から読み出し、当該出力データの印刷出力を行う出力部と、
を備えることを特徴とする画像形成装置。
【請求項２】
前記第２制御部は、累積印刷枚数が制限枚数を超えているか否かに基づいて、印刷が可能か否かを判断することを特徴とする請求項１に記載の画像形成装置。
【請求項３】
前記累積印刷枚数及び前記制限枚数は、ユーザ毎に設定されていることを特徴とする請求項２に記載の画像形成装置。
【請求項４】
ユーザ毎に印刷枚数を管理するための印刷管理テーブルを記憶する記憶部を備え、

前記第１制御部は、印刷出力する毎にユーザ認証を行い、当該認証されたユーザの印刷枚数を前記印刷管理テーブルに加算して印刷管理することを特徴とする請求項１に記載の画像形成装置。

【請求項５】

前記第１制御部による印刷管理の際に行われるユーザ認証は、パスワードによる第１の認証方法と、前記第１のユーザの認証情報を用いた第２の認証方法とのうち、どちらか一方の認証方法を選択可能であることを特徴とする請求項４に記載の画像形成装置。

【請求項６】

前記記憶媒体は、セキュリティキーであることを特徴とする請求項１～５の何れか一項に記載の画像形成装置。

【請求項７】

前記認証情報入力部は、印刷出力の開始を指示入力するためのスタートキーの指接触部分に設けられた指紋読取装置により構成されることを特徴とする請求項１～６の何れか一項に記載の画像形成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、入力データに基づいて印刷出力を行うファクシミリ装置、プリンタ、複写機又はこれらの複合機（以下、画像形成装置という。）に関する。

【０００２】

【従来の技術】

従来から、ユーザ端末において作成されたテキストデータや画像データを通信ネットワークを介して画像形成装置に送信し、画像形成装置において印刷出力するシステムが利用されている。このようなシステムでは、画像形成装置がユーザ端末から離れた場所に設置されていると、ユーザが画像形成装置のところへ印刷物を取りに行くまでに印刷物の内容を他人に見られたり、誤って印刷物を持っていかれたりする可能性が高く、重要な機密データを印刷する場合には情報が漏洩する恐れがあった。

【０００３】

ユーザ端末では、データのセキュリティを確保するために、セキュリティキーと呼ばれる記憶媒体が利用されている。このセキュリティキーには、個人の認証情報が記憶されており、ユーザ端末のＵＳＢポートにセキュリティキーを接続することにより、ユーザ端末ではセキュリティキーに記憶された認証情報に基づいて自動的にユーザ認証が行われる。しかしながら、セキュリティキーを用いてデータを保護できるのはユーザ端末においてのみであり、印刷時には通信ネットワーク上をデータが流れるため、画像形成装置ではセキュリティレベルが低下する。

【０００４】

画像形成装置でのセキュリティを向上させるために、親展機能を備えた画像形成装置も開発されている。これは、出力データにユーザＩＤやパスワード等のユーザの認証情報を付帯させてユーザ端末から画像形成装置に送信すると、画像形成装置で出力データが一時保存され、ユーザが画像形成装置の方へ出向いてユーザの認証情報を入力することで認証されたユーザのみが保存されている出力データを印刷出力することができるものである。

【０００５】

このユーザ認証時の方法も多数提案されており、例えば指紋読取装置を画像形成装置に備え、指紋情報によりユーザ認証を行う認証方法（例えば、特許文献１参照）や、ユーザＩＤが登録された登録カードを利用した認証方法（例えば、特許文献２参照）、ユーザの指紋情報が記憶されたＩＣ（Integrated Circuit）カードを利用した認証方法（例えば、特許文献３参照）等がある。

【０００６】

【特許文献１】

特開２００２－１０９５４２号公報

【特許文献２】
特開２００１－１６３８３号公報
【特許文献３】
特開２００１－２９７２８７号公報
【０００７】
【発明が解決しようとする課題】
しかしながら、上述したようなユーザＩＤや指紋情報等、ユーザ認証用に個人情報を利用する場合、予め画像形成装置にユーザの個人情報を登録しておかなければならず、その登録操作は煩雑であった。また、個人情報を画像形成装置に保存することは、個人情報のセキュリティの面から好ましくない。
【０００８】
さらに、パスワードを利用した一般的な認証方法は、ユーザがパスワードを暗記したり、パスワードを記録した手帳等を保管したりとパスワード管理が非常に煩雑である。
【０００９】
本発明の課題は、画像形成装置のセキュリティを向上させるとともに、ユーザ認証時の操作性を向上させることである。
【００１０】
【課題を解決するための手段】
請求項１に記載の発明は、画像形成装置において、
印刷出力対象の出力データ及びユーザの第１の認証情報が記憶された記憶媒体を接続するためのインターフェイス部と、
ユーザの第２の認証情報を入力する認証情報入力部と、
前記第１のユーザの認証情報及び前記第２の認証情報に基づいて、ユーザの認証を行う第１制御部と、
前記記憶媒体に記憶された出力データの印刷が可能か否かを判断する第２制御部と、
前記第１制御部によりユーザが認証され、かつ前記第２制御部により印刷可能と判断されると、前記記憶媒体に記憶された出力データを前記記憶媒体から読み出し、当該出力データの印刷出力を行う出力部と、
を備えることを特徴とする。
【００１１】
請求項２に記載の発明は、請求項１に記載の画像形成装置において、
前記第２制御部は、累積印刷枚数が制限枚数を超えているか否かに基づいて、印刷が可能か否かを判断することを特徴とする。
【００１２】
請求項３に記載の発明は、請求項２に記載の画像形成装置において、
前記累積印刷枚数及び前記制限枚数は、ユーザ毎に設定されていることを特徴とする。
【００１３】
請求項１～３に記載の発明によれば、セキュリティが低い通信ネットワークを経由することなく、データを印刷出力することができ、データの機密性を確保することができる。また、画像形成装置において認証された正規のユーザのみが印刷出力できるとともに、その認証情報としてユーザの個人情報を画像形成装置に登録しておく必要がないため、個人情報が漏洩する危険性がない。従って、画像形成装置のセキュリティを向上させることができる。
【００１６】
請求項４に記載の発明は、請求項１に記載の画像形成装置において、
ユーザ毎に印刷枚数を管理するための印刷管理テーブルを記憶する記憶部を備え、
前記第１制御部は、印刷出力する毎にユーザ認証を行い、当該認証されたユーザの印刷枚数を前記印刷管理テーブルに加算して印刷管理することを特徴とする。
【００１７】
請求項４に記載の発明によれば、ユーザの認証により、ユーザを特定することができ、認

証されたユーザ毎に印刷枚数を管理することができる。従って、印刷管理を正確かつ容易に行うことができる。

【００１８】

請求項５に記載の発明は、請求項４に記載の画像形成装置において、

前記第１制御部による印刷管理の際に行われるユーザ認証は、パスワードによる第１の認証方法と、前記第１のユーザの認証情報を用いた第２の認証方法とのうち、どちらか一方の認証方法を選択可能であることを特徴とする。

【００１９】

請求項５に記載の発明によれば、印刷管理のためにユーザの認証を行う際には、ユーザが記憶媒体を用いる機会が少ない場合はパスワードによる認証を選択する等、ユーザの状況に合わせて認証方法を選択でき、利便性が向上する。

【００２０】

請求項６に記載の発明は、請求項１～５の何れか一項に記載の画像形成装置において、

前記記憶媒体は、セキュリティキーであることを特徴とする。

【００２１】

請求項６に記載の発明によれば、ユーザ端末や他の外部装置においても使用可能なセキュリティキーによる認証方法を適用することにより、各装置間で一貫した認証方法でセキュリティを確保することができる。

請求項７に記載の発明は、請求項１～６の何れか一項に記載の画像形成装置において、

前記認証情報入力部は、印刷出力の開始を指示入力するためのスタートキーの指接触部分に設けられた指紋読取装置により構成されることを特徴とする。

請求項７に記載の発明によれば、印刷出力の指示と同時に指紋情報を入力することができ、操作性が良い。

【００２２】

【発明の実施の形態】

以下、図を参照して本発明の実施の形態を詳細に説明する。

【００２３】

〈第１の実施の形態〉

第１の実施の形態では、ユーザ端末において、ユーザの認証情報が登録されたセキュリティキーに印刷出力対象の出力データを保存し、当該セキュリティキーを画像形成装置に接続後、画像形成装置において、ユーザ認証を行い、ユーザが認証されるとセキュリティキーから出力データを読み出して印刷出力する印刷出力システムの例を説明する。なお、本実施の形態では、ユーザの認証情報としてユーザの指紋情報を適用した例を説明する。

【００２４】

まず、構成を説明する。

図１に、第１の実施の形態における印刷出力システム１００のシステム構成を示す。

図１に示すように、印刷出力システム１００は、ユーザ端末１０と、画像形成装置３０とが通信ネットワークＮを介して相互にデータの送受信が可能に接続され、ユーザ端末１０及び画像形成装置３０は、セキュリティキー２０を接続可能に構成されている。なお、図１には、１台のユーザ端末１０と、１台の画像形成装置３０とが接続された例を示したが、その設置台数及び設置場所は特に限定しない。

【００２５】

まず、ユーザ端末１０について説明する。

ユーザ端末１０は、指紋読取装置１０ａを備えて構成され、印刷出力時には、ユーザ端末１０で作成されたデータ（テキストデータ、画像データ含む）を印刷出力対象の出力データとしてセキュリティキー２０に格納する。

【００２６】

図２に、ユーザ端末１０の機能的構成を示す。

図２に示すように、ユーザ端末１０は、制御部１１、入力部１２、表示部１３、通信部１４、ＲＡＭ（Random Access Memory）１５、記憶部１６、インターフェイス（以下、Ｉ／

Ｆ；InterFaceという。）部１７、指紋読取装置１０ａを備えて構成される。
【００２７】
制御部１１は、ＣＰＵ（Central Processing Unit）等から構成され、記憶部１６に格納されるシステムプログラムの他、キー保存処理プログラム（図６参照）をＲＡＭ１５に展開し、当該プログラムとの協働により処理動作を統括的に制御する。
【００２８】
制御部１１は、キー保存処理において、指紋読取装置１０ａにより入力されたユーザの指紋情報と、セキュリティキー２０に記憶されている指紋情報とを照合し、ユーザ認証を行う。ユーザが認証されると、セキュリティキー２０に印刷出力対象の出力データを保存する。
【００２９】
入力部１２は、キーボードや、マウス等を備えて構成され、操作されたキーに対応する操作信号を制御部１１に出力する。
【００３０】
表示部１３は、ＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode Ray Tube）等から構成され、入力部１２からの入力情報や制御部１１による処理結果等の各種表示情報を表示する。
【００３１】
通信部１４は、ネットワークインターフェイスカード（以下、ＮＩＣ；Network Interface Cardという。）やモデム等の通信用のインターフェイスを備えて構成され、通信ネットワークＮ上の外部機器と相互に情報の送受信を行う。
【００３２】
ＲＡＭ１５は、制御部１１によって実行される各種プログラム及びこれらプログラムに係るデータを一時的に記憶するワークエリアを形成する。
【００３３】
記憶部１６は、磁気的又は光学的記録媒体、若しく半導体メモリから構成され、システムプログラムの他、キー保存処理プログラム及び各種プログラムで処理されたデータ等を記憶する。また、記憶部１６には、ユーザ端末１０において作成された画像データやテキストデータ等、印刷出力対象の出力データがデータベース化されて格納されている。
【００３４】
Ｉ／Ｆ部１７は、ユーザ端末１０とセキュリティキー２０とを接続するためのインターフェイスであり、ＵＳＢ（Universal Serial Bus）規格等が適用可能である。Ｉ／Ｆ部１７は、ユーザ端末１０とセキュリティキー２０との間で、データの転送速度や転送タイミングの調整を行い、両者間のデータのやりとりを仲介する。また、Ｉ／Ｆ部１７は、セキュリティキー２０が接続されると検出信号を制御部１１に出力する。
【００３５】
指紋読取装置１０ａは、ユーザの指紋を読み取り、その指紋情報をユーザ端末１０に入力する。なお、本実施の形態では、ユーザの認証情報として指紋情報を適用するので、指紋読取装置１０ａをユーザ端末１０に備えた例を説明するが、適用する認証情報に応じた認証情報入力装置をユーザ端末１０に備えればよい。例えば、認証情報として音声情報を適用する場合は、マイクをユーザ端末１０に備える。
【００３６】
次に、セキュリティキー２０について説明する。
セキュリティキー２０は、内部にＲＯＭ（Read Only Memory）を備えて、ユーザの認証情報やユーザ情報を記憶する記憶媒体である。なお、ユーザの認証情報及びユーザ情報は予めセキュリティキー２０に登録されていることとする。ユーザ情報には、ユーザＩＤ、ユーザ氏名、所属部署名等が含まれ、ユーザの認証情報としては、ユーザＩＤ、パスワード、指紋情報、音声情報等のユーザの身体情報等が適用可能であるが、これら以外の認証情報であってもよい。
【００３７】

また、セキュリティキー２０は、ＲＡＭを備え、このＲＡＭにユーザ端末１０により書き込まれた出力データを記憶する。
本実施の形態では、ユーザ１人がセキュリティキー１個を所有するものとして説明を行うが、これに限らず、グループ単位でセキュリティキー１個を共有することとしてもよい。
【００３８】
次に、画像形成装置３０について説明する。本実施の形態では、複写機能を有する画像形成装置の例を説明する。
画像形成装置３０は、入力データに基づいて印刷用紙に画像を形成して印刷出力するものであり、セキュリティキー２０に記憶されているユーザの認証情報を用いてユーザ認証を行い、ユーザが認証されると、セキュリティキー２０から出力データを読み出して印刷出力する。
【００３９】
図３に、画像形成装置３０の機能的構成を示す。
図３に示すように、画像形成装置３０は、制御部３１、認証情報入力部３０ａを有する入力部３２、表示部３３、記憶部３４、通信部３５、画像読取部３６、画像メモリ３７、出力部３８、Ｉ／Ｆ部３９を備えて構成される。
【００４０】
制御部３１は、ＣＰＵ等から構成され、記憶部３４に格納されるシステムプログラムの他、本発明に係る印刷出力処理プログラム（図７参照）、印刷管理処理プログラム（図８参照）等を図示しないＲＡＭに展開し、当該プログラムとの協働により処理動作を統括的に制御する。
【００４１】
制御部３１は、印刷出力処理において、Ｉ／Ｆ部３９を介して接続されるセキュリティキー２０に記憶されているユーザの指紋情報と、認証情報入力部３０ａから入力されたユーザの指紋情報とを照合して、ユーザ認証を行う。指紋情報が一致しており、ユーザが認証されると、セキュリティキー２０から出力データを読み出して画像メモリ３７に一時保存し、出力部３８に印刷出力を指示する。
【００４２】
また、印刷管理処理では、印刷出力の指示が入力されると、印刷出力処理時と同様に、Ｉ／Ｆ部３９を介して接続されるセキュリティキー２０に記憶されているユーザの指紋情報を用いてユーザ認証を行う。ユーザが認証されると、当該ユーザを特定し、記憶部３４に格納されている印刷管理テーブル３４１にユーザが登録されているか否かを判別する。ユーザが登録されていると、当該ユーザの累積印刷枚数は制限枚数を超えているか否かを判別し、超えていなければ出力部３８に印刷出力を指示し、今回の印刷枚数を印刷管理テーブル３４１に加算する。一方、印刷管理テーブル３４１にユーザが登録されていない場合、また登録されているがユーザの累積印刷枚数が制限枚数を超えている場合は、出力部３８に印刷出力の禁止を指示する。
【００４３】
入力部３２は、図４（ａ）に示すように、パスワード、ユーザＩＤ等のユーザの認証情報を入力するための数字キー３２１、印刷出力、画像読取等の画像形成動作の開始を指示するためのスタートキー３２２等の各種機能キーを備えて構成され、操作されたキーに対応する操作信号を制御部３１に出力する。
【００４４】
上記スタートキー３２２の指接触部分には、指紋読取装置から構成される認証情報入力部３０ａが併設される。具体的には、スタートキー３２２の指接触部分にコンタクトガラス３０１が形成され、その下部にスキャナ（図示せず）が設置される。図４（ｂ）に示すように、ユーザがスタートキー３２２を指で押下すると、押下した指の指紋が認証情報入力部３０ａにより読み取られて画像形成装置３０に入力される。なお、本実施の形態では、認証情報として指紋情報を適用するので、認証情報入力部３０ａが指紋読取装置から構成される例を説明するが、認証情報入力部３０ａは、適用する認証情報に応じた構成を適用

することとする。
【００４５】
また、入力部３２は、表示部３３と一体型に構成されるタッチパネル等を備え、タッチパネル上に表示された操作画面での入力操作に応じた操作信号を制御部３１に出力する。
【００４６】
表示部３３は、ＬＣＤ等から構成され、各種操作画面や制御部３１による処理結果等の各種表示情報を表示する。
【００４７】
記憶部３４は、磁気的又は光学的記録媒体、若しくは半導体メモリから構成され、システムプログラムの他、印刷出力処理プログラム、印刷管理処理プログラム及び各種プログラムで処理されたデータ等を記憶する。
【００４８】
また、記憶部３４は、ユーザ毎に印刷枚数を管理するための印刷管理テーブル３４１を内部に格納する。印刷管理テーブル３４１には、図５に示すように、ユーザ毎にユーザの所属グループ（例えば、“人事部”）、ユーザの累積印刷枚数（例えば、“２０”枚）、ユーザに対して設定されている制限枚数（例えば、“５０”枚まで）の各情報が格納されている。
【００４９】
通信部３５は、ＮＩＣやモデム等の通信用インターフェイスを備えて構成され、通信ネットワーク上の外部機器と相互にデータの送受信を行う。
【００５０】
画像読取部３６は、原稿台、原稿送り機構、スキャナ等から構成され、原稿台に載置された原稿を読み取ってデジタル画像データに変換し、当該画像データを画像メモリ３７に出力する。
【００５１】
画像メモリ３７は、印刷出力するデータを一時的に保存するメモリであり、画像読取部３６で読み取られた画像データ又はセキュリティキー２０から読み出された出力データを一時保存する。
【００５２】
出力部３８は、制御部３１からの出力指示に従って、画像メモリ３７に格納されている画像データ又は出力データに基づいて、指定されたサイズの印刷用紙に印刷出力を行う。その出力方式は、電子写真方式、インクジェット方式等、どの方式であってもよく、特に限定しない。
【００５３】
Ｉ／Ｆ部３９は、画像形成装置３０とセキュリティキー２０とを接続するためのインターフェイスであり、ＵＳＢ規格等が適用可能である。Ｉ／Ｆ部３９は、画像形成装置３０とセキュリティキー２０との間で、データの転送速度や転送タイミングの調整を行い、両者間のデータのやりとりを仲介する。また、Ｉ／Ｆ部３９は、セキュリティキー２０が接続されると検出信号を制御部３１に出力する。
【００５４】
次に、第１の実施の形態における動作を説明する。
第１の実施の形態では、ユーザ端末１０において出力データをセキュリティキー２０に保存し、ユーザがこのセキュリティキー２０を携帯して画像形成装置３０方へ移動し、当該画像形成装置３０にセキュリティキー２０を接続してセキュリティキー２０に保存された出力データを印刷出力する例を説明する。
【００５５】
まず、図６を参照して、ユーザ端末１０において実行されるキー保存処理を説明する。このキー保存処理は、ユーザ端末１０において印刷出力対象の出力データをセキュリティキー２０に保存する処理である。説明の前提として、ユーザにより出力データの印刷出力が指示され、印刷メニューからセキュリティキー２０を利用する印刷が選択されていること

とする。

【００５６】

図６に示すキー保存処理では、ステップＳ１において、制御部１１により、Ｉ／Ｆ部１７から出力される検出信号に基づいて、セキュリティキー２０がユーザ端末１０に接続されているか否かが判別される。Ｉ／Ｆ部１７から検出信号が出力されておらず、セキュリティキー２０が接続されていないと判別された場合は（ステップＳ１；Ｎ）、セキュリティキー２０を接続するよう促すガイダンスが行われる（ステップＳ２）。ガイダンスが終了すると、ステップＳ１に戻りセキュリティキー２０の接続が待機される。

【００５７】

Ｉ／Ｆ部１７から検出信号が出力され、セキュリティキー２０が接続されていると判別されると（ステップＳ１；Ｙ）、表示部１３に「認証のために指紋を読み取ります。指紋読取装置に指で触れて下さい」等のメッセージが表示され、ユーザの認証情報を入力するようガイダンスが行われる。指紋読取装置１０ａにより、ユーザの指紋が読み取られ、その指紋情報が入力されると（ステップＳ３）、セキュリティキー２０に登録されているユーザの指紋情報が読み出され、当該セキュリティキー２０に登録されているユーザの指紋情報と、指紋読取装置１０ａから入力された指紋情報とが照合され、一致するか否かが判別される（ステップＳ４）。

【００５８】

指紋情報が一致しないと判別された場合（ステップＳ４；Ｎ）、ユーザは認証されなかったとして、記憶部１６に格納されている出力データへのアクセスが禁止され（ステップＳ５）、本処理を終了する。

【００５９】

一方、指紋情報が一致すると判別された場合（ステップＳ４；Ｙ）、ユーザが認証されたとして、記憶部１６に格納されている出力データへのアクセスが許可され（ステップＳ６）、記憶部１６から出力データが読み出される。次いで、読み出された出力データがセキュリティキー２０に保存され（ステップＳ７）、保存が終了すると、本処理を終了する。

【００６０】

ユーザは、出力データが保存されたセキュリティキー２０を持って画像形成装置３０の方へ移動し、画像形成装置３０にセキュリティキー２０を接続する。

【００６１】

次に、図７を参照して、画像形成装置３０により実行される印刷出力処理を説明する。この印刷出力処理は、セキュリティキー２０に保存された出力データを読み出して印刷出力する処理である。

【００６２】

図７に示す印刷出力処理では、ステップＴ１において、Ｉ／Ｆ部３９から出力される検出信号に基づいて、セキュリティキー２０が画像形成装置３０に接続されているか否かが制御部３１により判別される。Ｉ／Ｆ部３９から検出信号が出力されており、セキュリティキー２０が接続されていると判別されると（ステップＴ１；Ｙ）、ユーザによるスタートキー３２２の押下が待機され、ステップＴ２では、ユーザによりスタートキー３２２が押下され、印刷出力が指示されたか否かが判別される。

【００６３】

スタートキー３２２が押下されると（ステップＴ２；Ｙ）、スタートキー３２２に併設されている認証情報入力部３０ａにより、ユーザの指紋が読み取られ、その指紋情報が入力される（ステップＴ３）。次いで、ステップＴ４では、セキュリティキー２０に登録されているユーザの指紋情報が読み出され、当該セキュリティキー２０に登録されているユーザの指紋情報と、認証情報入力部３０ａにより入力された指紋情報とが照合され、一致するか否かが判別される。

【００６４】

指紋情報が一致しないと判別された場合（ステップＴ４；Ｎ）、ユーザは認証されなかったとして、セキュリティキー２０に保存されている出力データへのアクセスが禁止される

（ステップＴ５）。そして、ユーザの認証エラーを通知するメッセージが表示部３３に表示され、本処理を終了する。

【００６５】

一方、指紋情報が一致すると判別された場合（ステップＴ４；Ｙ）、セキュリティキー２０に保存されている出力データへのアクセスが許可され（ステップＴ６）、セキュリティキー２０から出力データが読み出される。次いで、ステップＴ７では、読み出された出力データが出力部３８により印刷出力され、本処理を終了する。

【００６６】

次に、図８を参照し、上述した印刷出力処理とは別タスクで画像形成装置３０により実行される印刷管理処理を説明する。この印刷管理処理は、印刷出力を行うたびにセキュリティキー２０によりユーザを認証及び特定し、当該特定されたユーザ毎に印刷管理を行う処理である。

【００６７】

図８に示す印刷管理処理では、ステップＰ１において、Ｉ／Ｆ部３９から出力される検出信号に基づいて、セキュリティキー２０が画像形成装置３０に接続されているか否かが判別される。Ｉ／Ｆ部３９から検出信号が出力されており、セキュリティキー２０が接続されていると判別されると（ステップＰ１；Ｙ）、ユーザによるスタートキー３２２の押下が待機され、ステップＰ２では、ユーザによりスタートキー３２２が押下され、セキュリティキー２０に記憶された出力データの印刷出力指示、或いは複写モードでの印刷指示等、印刷出力が指示されたか否かが判別される。

【００６８】

スタートキー３２２が押下されると（ステップＰ２；Ｙ）、スタートキー３２２に併設されている認証情報入力部３０ａにより、ユーザの指紋が読み取られ、その指紋情報が入力される（ステップＰ３）。次いで、ステップＰ４では、セキュリティキー２０に登録されているユーザの指紋情報が読み出され、当該セキュリティキー２０に登録されているユーザの指紋情報と、認証情報入力部３０ａから入力された指紋情報とが照合され、一致するか否かが判別される。

【００６９】

指紋情報が一致しないと判別された場合（ステップＰ４；Ｎ）、ユーザは認証されなかったとして、画像形成装置３０における印刷出力が禁止される（ステップＰ５）。そして、ユーザの認証エラーが表示部３３に表示され、本処理を終了する。

【００７０】

一方、指紋情報が一致すると判別された場合（ステップＰ４；Ｙ）、ユーザは認証されたとして、セキュリティキー２０に記憶されている各種データへのアクセスが許可され、セキュリティキー２０からユーザ情報が読み出されて、認証されたユーザが特定される（ステップＰ６）。

【００７１】

次いで、ステップＰ７では、特定されたユーザが印刷管理テーブル３４１にユーザ登録されているか否かが判別される。印刷管理テーブル３４１にユーザ登録されていない場合（ステップＰ７；Ｎ）、指示に応じた印刷出力が行われる（ステップＰ８）。例えば、複写モードで印刷出力が指示された場合は、画像読取部３６により原稿の画像データが読み取られ、出力部３８により画像データが印刷出力される。また、セキュリティキー２０に記憶された出力データの印刷出力が指示された場合は、上記印刷出力処理で説明したように、セキュリティキー２０から出力データが読み出されて印刷出力される。

【００７２】

一方、印刷管理テーブル３４１にユーザ登録されている場合（ステップＰ７；Ｙ）、当該印刷管理テーブル３４１が参照され、特定されたユーザの累積印刷枚数は制限枚数を超えているか否かが判別される（ステップＰ９）。累積印刷枚数が制限枚数を超えていると判別された場合は（ステップＰ９；Ｙ）、ステップＰ５に移行し、ユーザによる印刷出力が禁止される。このとき、表示部３３に「制限枚数を超えているため、印刷出力できません

。」等のメッセージが表示され、本処理を終了する。

【００７３】

ユーザの累積印刷枚数が制限枚数を超えていないと判別された場合（ステップＰ９；Ｎ）、ユーザによる印刷出力が許可され（ステップＰ１０）、指示に応じた印刷出力が行われる（ステップＰ１１）。次いで、今回の印刷出力でカウントされた印刷枚数が印刷管理テーブル３４１の累積印刷枚数に加算され（ステップＰ１２）、本処理を終了する。

【００７４】

以上のように、第１の実施の形態では、ユーザ端末１０において印刷出力対象の出力データがセキュリティキー２０に保存され、このセキュリティキー２０を画像形成装置３０に接続すると、画像形成装置３０ではセキュリティキー２０に登録されているユーザの認証情報を用いてユーザ認証が行われ、ユーザが認証されると保存された出力データが印刷出力されるので、セキュリティが低い通信ネットワークを経由することなく、ユーザ端末１０で作成された出力データ画像形成装置において印刷出力することができ、データの機密性を確保することができる。

【００７５】

また、画像形成装置３０に認証情報入力部３０ａを備え、ユーザ認証時には認証情報入力部３０ａから入力された認証情報と、セキュリティキー２０に登録されている認証情報とを照合してユーザ認証を行うので、認証された正規のユーザのみセキュリティキー２０に記憶されている出力データの印刷出力を行うことができ、画像形成装置３０のセキュリティを向上させることができる。

【００７６】

また、認証時に指紋情報を読み取る認証情報入力部３０ａは、スタートキー３２２に併設されているので、印刷出力の指示入力と同時に指紋情報を入力することができ、操作性が良い。

【００７７】

また、セキュリティキー２０に登録されているユーザの認証情報を用いて、ユーザ端末１０で記憶されている出力データへのアクセス、セキュリティキー２０に保存されている出力データへのアクセスを制限するので、ユーザ端末１０におけるデータ管理から画像形成装置３０における印刷出力まで、一貫した認証方法でセキュリティを確立することができるとともに、複数段階でユーザ認証が行われ、よりセキュリティが向上する。

【００７８】

また、従来は画像形成装置３０にユーザ認証用の個人情報を登録することにより、個人情報が外部へ漏洩する危険性があったが、本発明ではユーザ認証用の個人情報を画像形成装置３０に登録する必要がなく、個人情報漏洩の問題が生じない。また、ユーザの認証情報を登録する登録操作を省略することができる。

【００７９】

また、セキュリティキー２０によりユーザを認証するとともにユーザの特定を行い、当該特定されたユーザの印刷管理を行うので、認証されたユーザ毎に印刷管理を行うことができ、より利便性が向上する。

【００８０】

〈第２の実施の形態〉

第２の実施の形態では、画像形成装置において、原稿から読み取られた画像データを外部へ持ち出す際に、当該画像データをセキュリティキーに保存することにより、データの機密性を確保する例を説明する。

【００８１】

まず、第２の実施の形態における画像形成装置の構成について説明するが、第２の実施の形態における画像形成装置の構成は、第１の実施の形態で説明した画像形成装置３０と同一であるので、その図示を省略し、異なる機能部分についてのみ説明する。すなわち、第２の実施の形態における画像形成装置３０は、制御部３１、認証情報入力部３０ａを有する入力部３２、表示部３３、記憶部３４、通信部３５、画像読取部３６、画像メモリ３７

、出力部３８、Ｉ／Ｆ部３９を備えて構成される。
【００８２】
制御部３１は、記憶部３４から本発明に特徴的なデータ保存処理プログラム（図９参照）を読み出して、当該プログラムとの協働により処理動作を統括的に制御する。
【００８３】
制御部３１は、後述するデータ保存処理において、スタートキー３２２が押下され、画像読取を指示されると、Ｉ／Ｆ部３９を介して接続されるセキュリティキー２０に登録されている指紋情報と、認証情報入力部３０ａから入力された指紋情報とを照合し、ユーザ認証を行う。ユーザが認証されると、画像読取部３６に読み取りを指示し、画像読取部３６により読み取られた画像データをセキュリティキー２０に保存する。
【００８４】
記憶部３４は、上記データ保存処理プログラムを内部に格納する。
【００８５】
次に、第２の実施の形態における動作について説明する。
図９を参照して、画像形成装置３０により実行されるデータ保存処理について説明する。このデータ保存処理は、原稿から読み取られた画像データをセキュリティキー２０に保存する処理である。説明の前提として、操作メニューからデータ保存処理が選択され、以下の処理が開始されたこととする。
【００８６】
図９に示すデータ保存処理では、まずステップＥ１において、Ｉ／Ｆ部３９から出力される検出信号に基づいて、セキュリティキー２０が画像形成装置３０に接続されているか否かが判別される。Ｉ／Ｆ部３９から検出信号が出力されておらず、セキュリティキー２０が接続されていないと判別された場合（ステップＥ１；Ｎ）、セキュリティキー２０を画像形成装置３０に接続するよう促すガイダンスが行われる（ステップＥ２）。ガイダンス後、ステップＥ１に戻りセキュリティキー２０の接続が待機される。
【００８７】
Ｉ／Ｆ部３９から検出信号が出力され、セキュリティキー２０が接続されていると判別されると（ステップＥ１；Ｙ）、ユーザによるスタートキー３２２の押下が待機され、ステップＥ３では、ユーザによりスタートキー３２２が押下され、画像読取開始が指示されたか否かが判別される。
【００８８】
スタートキー３２２が押下されると（ステップＥ３；Ｙ）、スタートキー３２２に併設されている認証情報入力部３０ａにより、ユーザの指紋が読み取られ、その指紋情報が入力される（ステップＥ４）。次いで、セキュリティキー２０に登録されているユーザの指紋情報が読み出され、当該セキュリティキー２０に登録されているユーザの指紋情報と、認証情報入力部３０ａにより読み取られた指紋情報とが照合され、一致するか否かが判別される（ステップＥ５）。
【００８９】
指紋情報が一致しないと判別された場合（ステップＥ５；Ｎ）、ユーザが認証されなかったとして、セキュリティキー２０へのデータ保存が禁止される（ステップＥ６）。
【００９０】
一方、指紋情報が一致したと判別された場合（ステップＥ５；Ｙ）、ユーザは認証されたとして、セキュリティキー２０へのデータ保存が許可される（ステップＥ７）。次いで、画像読取部３６により原稿台に載置された原稿の読み取りが行われ（ステップＥ８）、原稿から読み取られた画像データがセキュリティキー２０に保存される（ステップＥ９）。セキュリティキー２０において画像データの保存が終了すると、本処理を終了する。
【００９１】
ユーザは、データが保存されたセキュリティキー２０を持ってユーザが所有するユーザ端末１０にセキュリティキー２０を接続してデータをユーザ端末１０に転送することもできるし、異なる場所に設置されている画像形成装置３０に接続して印刷出力することもで

きる。

【００９２】

なお、第２の実施の形態においても、画像形成装置３０により印刷管理処理が実行されるが、第２の実施の形態における印刷管理処理は、第１の実施の形態における印刷管理処理（図８参照）と同様であるので、その説明は省略する。

【００９３】

以上のように、第２の実施の形態では、画像形成装置３０において、セキュリティキー２０に登録されているユーザの認証情報を用いてユーザ認証を行い、当該ユーザが認証されると、画像読取部３６により読み取られた画像データをセキュリティキー２０に保存するので、通信ネットワークを経由することなく、画像形成装置３０において読み取った画像データを他の外部装置に入力することができ、データの機密性を確保することができる。

【００９４】

また、画像形成装置３０に認証情報入力部３０ａを備え、ユーザ認証時には認証情報入力部３０ａから入力された認証情報と、セキュリティキー２０に登録されている認証情報とを照合してユーザ認証を行うので、認証された正規のユーザのみセキュリティキー２０にデータを保存することができ、画像形成装置３０のセキュリティを向上させることができる。

【００９５】

また、認証時に指紋情報を読み取る認証情報入力部３０ａは、スタートキー３２２に併設されているので、原稿読み取りの指示入力と同時に指紋情報を入力することができ、操作性が良い。

【００９６】

また、セキュリティキー２０に保存された画像データを他の外部装置で読み出す際にもセキュリティキー２０に登録されているユーザの認証情報を用いて、ユーザ認証を行うことができるので、セキュリティキー２０を接続する装置が異なっても一貫した認証方法でセキュリティを確立することができる。

【００９７】

また、従来は画像形成装置３０にユーザ認証用の個人情報を登録することにより、個人情報が外部へ漏洩する危険性があったが、本発明ではユーザ認証用の個人情報を画像形成装置３０に登録する必要がなく、個人情報漏洩の問題が生じない。さらに、ユーザの認証情報を登録する登録操作を省略することができる。

【００９８】

また、セキュリティキー２０によりユーザを認証するとともにユーザの特定を行い、当該特定されたユーザの印刷管理を行うので、認証されたユーザ毎に印刷管理を行うことができ、より利便性が向上する。

【００９９】

なお、上述した第１及び第２の実施の形態における記述内容は、本発明を適用した画像形成装置３０の好適な一例であり、これに限定されない。

例えば、上述した説明では、出力データを記憶する記憶媒体としてセキュリティキーを適用した場合を説明したが、これに限らず、カード状、スティック状等の各種形状の小型メモリや、ＩＣチップを搭載したＩＣカード等を適用することとしてもよい。

【０１００】

また、上述した印刷管理処理では、印刷管理を行うユーザを特定するためにセキュリティキー２０を用いた認証方法でユーザ認証を行う例を示したが、ユーザ認証は、パスワードを用いる第１の認証と、セキュリティキー２０を用いる第２の認証とのうち、どちらか一方を印刷管理テーブル３４１にユーザ登録する際に選択可能であるとする。ユーザによっては画像形成装置３０を利用する際には複写機能を使用する場合が多く、セキュリティキー２０を用いる機会が少ない場合があるので、このようなユーザの場合はパスワードによる第１の認証を選択することにより、認証操作が容易になる。

【０１０１】

また、印刷管理テーブル３４１を画像形成装置３０に備えて各ユーザの印刷管理を行うこととしたが、セキュリティキー２０に、そのセキュリティキー２０を所有するユーザの累積印刷枚数、制限枚数を記憶して印刷管理することとしてもよい。

【０１０２】

その他、本実施の形態における画像形成装置３０の細部構成及び細部動作に関しても適宜変更可能である。

【０１０３】

【発明の効果】

請求項１～３に記載の発明によれば、セキュリティが低い通信ネットワークを経由することなく、データを印刷出力することができ、データの機密性を確保することができる。また、画像形成装置において認証された正規のユーザのみが印刷出力できるとともに、その認証情報としてユーザの個人情報を画像形成装置に登録しておく必要がないため、個人情報が漏洩する危険性がない。従って、画像形成装置のセキュリティを向上させることができる。

【０１０６】

請求項４に記載の発明によれば、ユーザの認証により、ユーザを特定することができ、認証されたユーザ毎に印刷枚数を管理することができる。従って、印刷管理を正確かつ容易に行うことができる。

【０１０７】

請求項５に記載の発明によれば、印刷管理のためにユーザの認証を行う際には、ユーザが記憶媒体を用いる機会が少ない場合はパスワードによる認証を選択する等、ユーザの状況に合わせて認証方法を選択でき、利便性が向上する。

【０１０８】

請求項６に記載の発明によれば、ユーザ端末や他の外部装置においても使用可能なセキュリティキーによる認証方法を適用することにより、各装置間で一貫した認証方法でセキュリティを確保することができる。

請求項７に記載の発明によれば、印刷出力の指示と同時に指紋情報を入力することができ、操作性が良い。

【図面の簡単な説明】

【図１】本発明を適用した第１の実施の形態の印刷出力システムのシステム構成を示す図である。

【図２】ユーザ端末の機能的構成を示す図である。

【図３】画像形成装置の機能的構成を示す図である。

【図４】数字キーと、認証情報入力部が併設されたスタートキーとを示す図である。

【図５】第３の実施の形態における画像形成装置の記憶部に記憶される印刷管理テーブルのデータ構成を示す図ある。

【図６】ユーザ端末により実行されるキー保存処理を説明するフローチャートである。

【図７】画像形成装置により実行される印刷出力処理を説明するフローチャートである。

【図８】画像形成装置により実行される印刷管理処理を説明するフローチャートである。

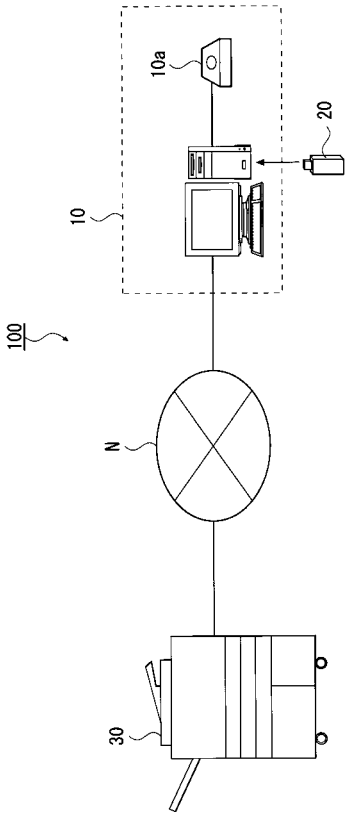
【図９】第２の実施の形態における画像形成装置により実行されるデータ保存処理を説明するフローチャートである。

【符号の説明】

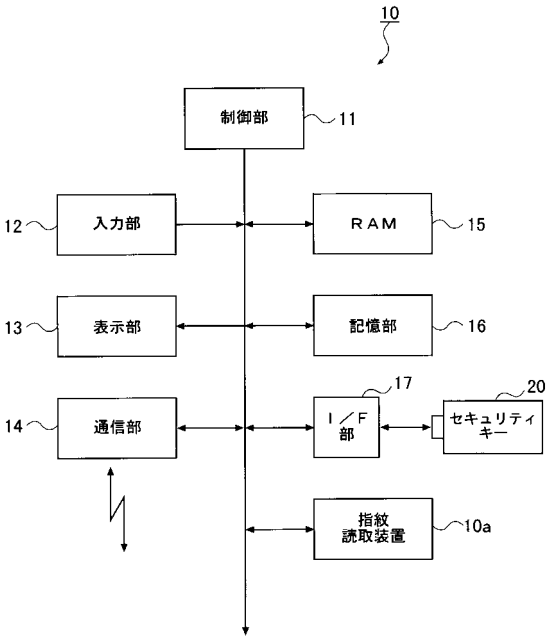
１００　印刷出力システム
１０　ユーザ端末
１０ａ　指紋読取装置
１１　制御部
１２　入力部
１３　表示部
１４　通信部
１５　ＲＡＭ

１６　記憶部
１７　Ｉ／Ｆ部
２０　セキュリティキー
３０　画像形成装置
３１　制御部
３２　入力部
３０ａ　認証情報入力部
３３　表示部
３４　記憶部
３４１　印刷管理テーブル
３５　通信部
３６　画像読取部
３７　画像メモリ
３８　出力部
３９　Ｉ／Ｆ部

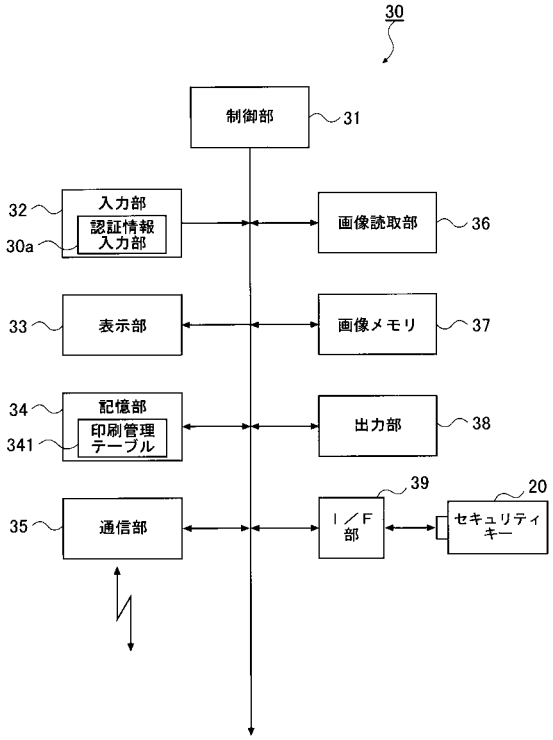
【図１】



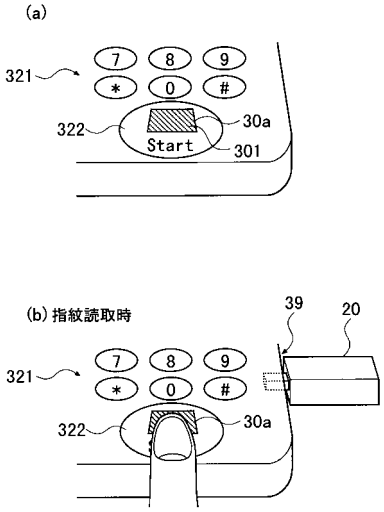
【図２】



【図３】



【図４】

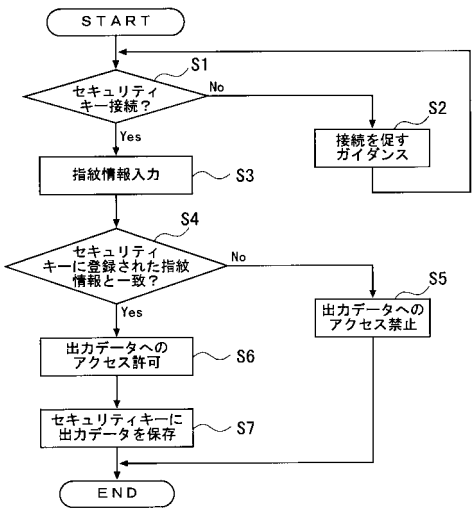


【図５】

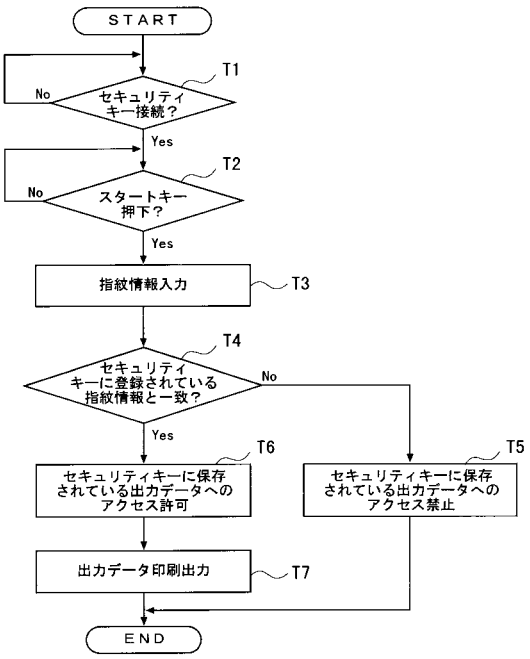
341

ユーザ	所属グループ	累積印刷枚数	制限枚数
ユーザA	人事部	２０	５０
ユーザB	総務部	３５	２００
⋮	⋮	⋮	⋮

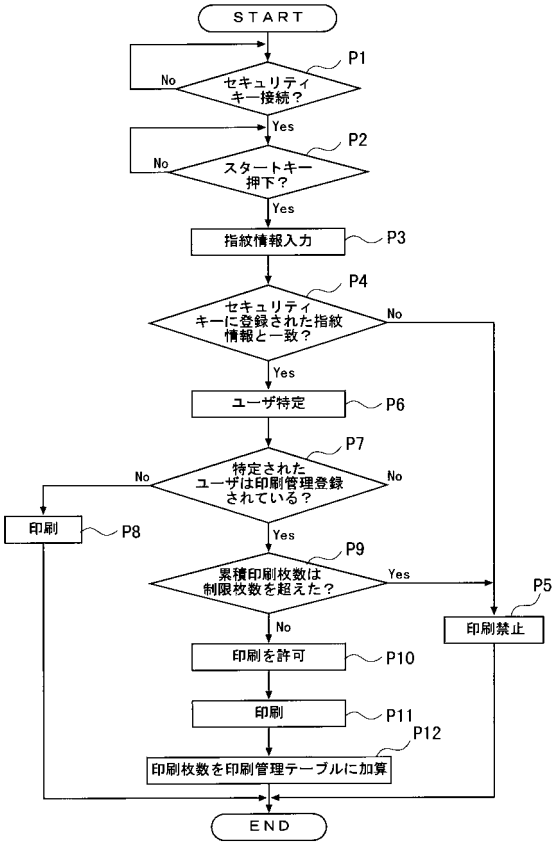
【図６】



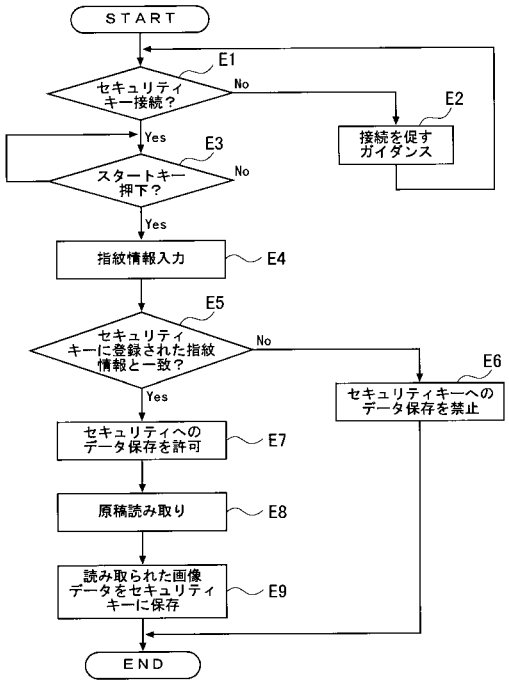
【図７】


START
T1
No
セキュリティキー接続？
Yes
T2
No
スタートキー押下？
Yes
指紋情報入力
T3
T4
セキュリティキーに登録されている指紋情報と一致？
No
Yes
T6
セキュリティキーに保存されている出力データへのアクセス許可
T5
セキュリティキーに保存されている出力データへのアクセス禁止
出力データ印刷出力
T7
END

【図８】


START
P1
No
セキュリティキー接続？
Yes
P2
No
スタートキー押下？
Yes
指紋情報入力
P3
P4
セキュリティキーに登録された指紋情報と一致？
No
Yes
ユーザ特定
P6
P7
No
特定されたユーザは印刷管理登録されている？
No
Yes
印刷
P8
P9
累積印刷枚数は制限枚数を超えた？
Yes
P5
印刷禁止
No
印刷を許可
P10
印刷
P11
P12
印刷枚数を印刷管理テーブルに加算
END

【図９】


START
E1
セキュリティキー接続？
No
E2
接続を促すガイダンス
Yes
E3
スタートキー押下？
No
Yes
指紋情報入力
E4
E5
セキュリティキーに登録された指紋情報と一致？
No
E6
セキュリティキーへのデータ保存を禁止
Yes
セキュリティへのデータ保存を許可
E7
原稿読み取り
E8
読み取られた画像データをセキュリティキーに保存
E9
END

フロントページの続き

(72)発明者　泉　賀津雄
東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内
(72)発明者　青山　素明
東京都八王子市石川町２９７０番地　コニカビジネステクノロジーズ株式会社内

審査官　内田　正和

(56)参考文献　特開平０６－１５３２７１（ＪＰ，Ａ）
特開平１０－１９１０７１（ＪＰ，Ａ）
特開２００１－２３６１９８（ＪＰ，Ａ）
特開２００１－１８８６６４（ＪＰ，Ａ）
特開２００２－１６３６２８（ＪＰ，Ａ）
特開２００２－１３７５０１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　3/12
B41J　5/30
B41J　29/38
G03G　21/04
H04N　1/00